REMARKS

Claims 1-44 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,249,582 by Gilley. Applicant respectfully submits that Gilley does not disclose each and every element of the invention as claimed in claims 1-44.

Gilley discloses shortening the length of an initial initialization vector (IV) to less than the bit length of each block of information processed by a block cipher, thus reducing the overhead of the block cipher. In particular, Gilley discloses loading a 32-bit initial IV and 32 pseudo-random bits into a linear feedback shift register to calculate a 64-bit IV as an alternative to using a 64-bit initial IV. Gilley further discloses generating pseudo-random numbers in CBC mode by encrypting a 32-bit IV with 32 other values to create blocks of 32 bit pseudo-random numbers such that each succeeding pseudo-random number depends on the preceding number.

In contrast, independent claims 1, 8, 12, 19, 23, 30, 34, and 41 recite deriving a calculated IV from each string of data from each stride. Gilley's loading a 32-bit initial IV and 32 pseudo-random bits into a linear feedback shift register is not equivalent to deriving a calculated IV from each string of data from each stride as claimed. Gilley does not teach or suggest that either the initial IV or the pseudo-random bits are chosen from each string of data from each stride.

Furthermore, by making successive pseudo-random numbers dependent on the preceding numbers, Gilley discloses an initial IV being carried over to successive pseudo-random numbers. Carrying over an initial IV while encrypting successive strides is not equivalent to deriving a calculated IV from each string of data from each stride as claimed.

Accordingly, Applicant respectfully submits that independent claims 1, 8, 12, 19, 23, 30, 34, and 41 and associated claims 2-7, 9-11, 13-18, 20-22, 24-29, 31-33, and 35-44 are not anticipated by Gilley under 35 U.S.C. § 102(b) and respectfully requests the withdrawal of the rejection.

SUMMARY

In view of the foregoing remarks, Applicant respectfully submits that the pending claims 1-44 are in condition for allowance. If the Examiner determines the prompt allowance of these claims could be facilitated by a telephone conference, the Examiner is invited to contact Sue Holloway at (408) 720-8300 x309.
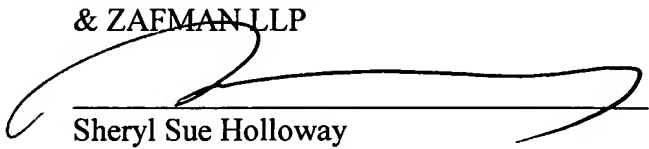
Deposit Account Authorization

Authorization is hereby given to charge our Deposit Account No. 02-2666 for any charges that may be due. Furthermore, if an extension is required, then Applicant hereby requests such extension.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: April 12, 2005

Sheryl Sue Holloway
Attorney for Applicant
Registration No. 37,850

12400 Wilshire Boulevard, Seventh Floor
Los Angeles, CA 90025-1026
(408) 720-8300